AUTHENTICATION AND VERIFICATION OF WEB PAGE CONTENT

ABSTRACT

Authentication and verification of the integrity of multimedia content delivered from a server to a client through a computer network, such as the Internet, provides a substantial reduction in the possibility of inaccurate and/or unintended content being displayed to a user. Each content file stored on the server is cryptographically registered and such registration information is stored on the server along with the corresponding file name. A user is provided with a second (e.g., public) key corresponding to a first (e.g., private) key used to cryptographically register the content files.

Through a consumer application such as a Web browser, the user instructs the client to request Web content from the server. The server assembles a list of the content files necessary to satisfy the request and transmits the list to the client. Prior to transmitting the actual content files, the server transmits to the client the registration information for these content files. The client uses the second key to validate the cryptographic registration information for any listed content files already resident locally. If the registration information for any files can be successfully validated, then those files have been authenticated and verified and do not need to be transmitted from the server. The server then transmits the actual content files for those files not yet authenticated and verified at the client. The client again uses the second key to validate the cryptographic registration information for the content files received from the server. If the registration information for all of the files is successfully validated, then the client displays the Web page. If any files cannot be successfully validated, then the client will not display any portion of the Web page.